State of Kansas

Information Technology

Security Policies

&

Guidelines

PUBLISHED BY:

KANSAS INFORMATION TECHNOLOGY EXECUTIVE COUNCIL

AUGUST, 2001

1. Introduction 5
1.1 General Policy Statement 5
1.2 Scope 5
1.3 Compliance 5
1.4 Document Changes and Feedback 6
2. Organizational Roles & Responsibilities 6
2.1 Agency Head 6
2.2 Data Owners 6
2.3 Custodians 6
2.4 Users 7
2.5 Security Administration 7
2.6 System Administration 7
2.7 Database Administration 7
2.8 Computer and Network Operations 8
2.9 Application System Development 8
2.10 Legislative Auditor 8
2.11 Risk Analysis 8
3. Vendor/Contractor Relationships 8
4. Security Incident Reporting 8
5. Application & System Security Planning Process for Development or Modification 9
5.1 Projects which DO NOT Require State of Kansas Resources, Systems or Network Connections 9
5.2 Projects which Require State of Kansas Resources, Systems, or Network Connections 9
5.3 Security Implications for System Development and Testing 10
6. Information Security 11
6.1 Authorized Use and Ownership of Information Resources 11
6.2 Availability of Critical Data & Systems 11
6.3 User Accountability: Userids and Passwords 12
6.4 Access Controls 12
6.5 Authorization 13
6.6 Audit Trails 13
6.7 Application Security 14

6.8 Adapting Policies and Procedures ____ **14**

7. Authentication, Data Encryption & Key Management ____ ***14***

7.1 Authentication ____ **14**

7.2 Devices ____ **14**

7.3 Services ____ **15**

7.4 Encryption ____ **15**

7.5 Encryption Requirements ____ **15**

7.6 Encryption Services ____ **16**

7.7 Considerations for Data Encryption Systems ____ **16**

7.8 Encryption and Authentication Keys ____ **17**

7.9 Key Management ____ **17**

7.10 Data and File Encryption ____ **17**

7.11 Guidelines for data and file encryption: ____ **17**

8. Network Security Policies ____ ***18***

8.1 General Network Controls ____ **18**

8.2 Distributed Network Access Security ____ **19**

8.3 Guidelines for distributed network access: ____ **19**

8.4 Network connectivity and Monitoring Controls ____ **20**

8.5 System Identification Screens ____ **21**

8.6 Guidelines for system identification screens: ____ **21**

9. Personal Computers and State of Kansas Equipment Policies & Guidelines ____ ***21***

9.1 Practices ____ **21**

9.1.1 Information Security ____ 21
9.1.2 Visual Displays: ____ 22
9.1.3 Wireless Transmissions: ____ 22
9.1.4 Passwords ____ 22
9.1.5 Computer and Network Security ____ 22
9.1.6 Anti-virus Software: ____ 23
9.1.7 Data backup and Storage: ____ 23
9.1.8 Portable Computers: ____ 23
9.1.9 Remote Access: ____ 23
9.1.10 Diagnostic and Monitoring Tools: ____ 24
9.1.11 External Systems ____ 24
9.1.12 Software and Licensing ____ 24
9.1.13 Privacy ____ 24
9.1.14 Security Incident Reporting ____ 24

10. Physical Security ____ ***24***

10.1 Access control measures: ____ **25**

10.2 Fire Suppression Measures ____ **25**

10.3 Environmental Measures. ____ **26**

10.4 Electrical Power Measures 26
10.5 Office space 27
11. Issue-Specific Policies *27*
11.1 User Responsibilities 27
11.2 Internet Access 27
11.2.1 Monitoring Internet Access 28
11.3 E-mail 28
11.4 Voice Mail Systems 29
11.5 Remote Access 29
11.6 Video 29
11.7 Virus Protection 30
Appendix A: Security Acknowledgement *32*
Appendix B: Glossary of Terms *33*

1. Introduction

The purpose of this document is to provide guidance on Statewide Information Technology Security Policies that apply to all State of Kansas computing and network environments. If there is a conflict between this document and another State of Kansas policy document, the document with the more stringent control takes precedence.

The foundations of this policy are the security concepts of:

- Business need-to-know;
- Least privilege;
- Separation of duties;
- Risk Management;
- Accountability; and
- Auditability.

This document should be used as a template for a starting point in the developing of an agency Security Policy or Guideline. State agencies should review this document, along with the Kansas State Technical Architecture, and use them to create individual agency security policies that meet the specific needs of their environment.

Agencies are also cautioned that documents of this type are considered Open Records. Therefore, sensitive security related details should be maintained in a separate, non-public security procedure manual.

1.1 General Policy Statement

Information is a State of Kansas asset requiring protection commensurate with its value. Measures must be taken to protect information from unauthorized modification, destruction, or disclosure whether accidental or intentional, as well as to assure its authenticity, integrity, availability, and confidentiality.

1.2 Scope

The controls in this document are the minimum requirements for providing a secure environment for developing, implementing, and maintaining systems.

This document applies to all State of Kansas entities, agents, employees, contractors, or vendors involved in the development, implementation, and maintenance of information systems.

1.3 Compliance

All State of Kansas employees, agents, contractors, and vendors are responsible for understanding and complying with all State of Kansas Information Technology Security Policies. This would include building and configuring systems in accordance with these policies. Non-compliant situations will be brought to the attention of management for appropriate action that may result in loss of network connectivity, disciplinary action, up to and including immediate dismissal and/or criminal prosecution.

Outsourced processing and storage facilities, such as service bureaus, vendors, partnerships, and alliances, must be monitored and reviewed to ensure either compliance

with State of Kansas policies, or that a level of control is provided which is equivalent to State of Kansas policies. This should be accomplished through contractual commitments with provisions to permit auditing and monitoring to ensure compliance.

All necessary exceptions to this policy must be clearly documented and approved by the agency head or designee.

1.4 Document Changes and Feedback

Agency Security Policies must be reviewed and updated annually. If there is a major change during the year, an addendum will be issued and communicated to managers for dissemination to appropriate personnel. Discrepancies should therefore be reported as soon as possible to the Agency security staff for review and inclusion in the next version or addendum.

2. Organizational Roles & Responsibilities

Information security requires the active support and ongoing participation of individuals from all departments and management levels of the organization. It requires support from the executive level and compliance from everyone.

The following are suggestions for specific roles and responsibilities both at the management and staff level. When roles and responsibilities are assigned, the “separation of duties” concept must be taken into consideration to ensure State of Kansas’s assets are adequately protected.

2.1 Agency Head

The agency head is ultimately responsible for carrying out the security policy at State of Kansas and for the development and implementation of the agency security plan.

2.2 Data Owners

Data owners are, by law, the person(s) responsible for collecting, ensuring protection of, and authorizing access to data.

The owner is responsible and authorized to:

- approve all access to resources under his or her responsibility;
- judge the asset’s value and label the data as such;
- Ensure compliance with applicable controls through regular review of data classification and authorized access.

2.3 Custodians

Custodians are responsible for the safety and integrity of data in their custody.
The custodian has responsibility to:

- implement the controls specified by the owner;
- provide safeguards for information resources;
- Administer access to the information resources and make provisions for timely detection, reporting, and analysis of unauthorized attempts to gain access to information resources.

2.4 Users

Users are all people who use State information assets for business purposes. The user must protect these information resources from unauthorized activities including disclosure, modification, deletion, and usage.
Users have the responsibility to:

- use the resource only for the purposes specified by its owner;
- comply with controls established by the owner or public law;
- Prevent disclosure of sensitive information.

2.5 Security Administration

The security administration function provides administration for user access to systems. These responsibilities include, but may not be limited to:

- authentication (add, change, delete) services to provide userids with logonids and passwords;
- authorization (add, change, delete) services to provide user access to applications;
- Generation and distribution of reports for monitoring access and potential security breaches.

2.6 System Administration

The system administration function monitors performance, provides problem determination, production support, and performs system back-ups. System Administration responsibilities can include, but may not be limited to, ensuring that:

- only authorized security software is installed via authorized means;
- approved security procedures are followed and procedures are established where necessary;
- systems are recovered in a secure manner;
- ad hoc system reviews are performed to identify unusual activity;
- systems are installed and operated using no less than the security controls provided by the vendor and using any security controls specified in the Corporation's applicable security policies;
- the security access administration function is notified of changes to software that might impact system security features before installation of those changes; and,
- Procedures for software license validation and virus testing have been followed.

2.7 Database Administration

The database administration (DBA) function at State of Kansas has responsibility for the proper administration of agency owned databases. DBAs are responsible for the development, maintenance, and integrity of these databases unless otherwise specified by the database owner. Security responsibilities include, but may not be limited to:

- designing, developing, organizing, managing, and controlling the database in accordance with security policies;
- providing the security access administration function with the necessary information to maintain user IDs and privileges; and,
- Recovering databases in a secure manner when damaged or compromised.

2.8 Computer and Network Operations

The computer and network operations functions are responsible for operating and managing information systems or networks in accordance with security policies, monitoring systems for signs of security violations, and following the escalation process for reporting security violations.

2.9 Application System Development

Application and system developers are responsible for ensuring that the systems he or she develops are created according to the State of Kansas security policies and any additional technical specifications that may apply.

2.10 Legislative Auditor

Legislative auditors evaluate compliance with the Information Technology Security Policy through periodic examinations of information systems and applications, including verification that the appropriate management processes have been effectively applied. They are to be given necessary access to corporate premises, personnel, system, and records needed to conduct their business.

2.11 Risk Analysis

Having Security Policies and guidelines is essential if an agency is to maintain a secure information resource environment. However, having these policies and guidelines is not enough. Those policies must be implemented to be effective and they must be periodically reviewed to continue to be effective. Therefore, it's important that periodic Risk Analysis program be implemented.

It is recommend that all agency security policies be approached on a step by step basis. The best starting point is an assessment of the current position, followed by identification of what changes are needed for compliance. Once that has been accomplished, planning and implementation must be undertaken.

3. Vendor/Contractor Relationships

Allowing access to State of Kansas information to anyone outside of State of Kansas may be necessary at times but this access must be carefully considered. There are occasions when vendors and contractors will require access to State of Kansas systems and State agencies must take precautions to protect all State of Kansas information.

4. Security Incident Reporting

There are several categories of information security incidents. Some examples are computer fraud, viruses, and network penetration. All suspected information security incidents must be reported as quickly as possible through the appropriate channels.

- All users must report suspected security breaches to their manager.
- Once notified, Managers must notify the appropriate security staff of the reported security incident.
- Managers are responsible for keeping upper management informed of security incidents.
- The security staff will investigate, research, resolve and document the event.
- The Security staff is responsible for:

- ensuring procedural documentation exists for handling information security incidents;
- review and analysis of the incident tracking database; and
- When necessary, keeping the State of Kansas network community informed of security incidents and possible precautions users should implement.

5. Application & System Security Planning Process for Development or Modification

A security plan is required for all projects involving development and implementation of new systems or modification to existing systems where there is a change in access or functionality. This includes pilot projects, proofs of concept, temporary access to production systems, and development environments. If an approved security plan already exists and changes are made to the technology used, network, access methods, controls, or classification of data, then an addendum is required.

The security plan should include, but is not limited to:

- Project Purpose and Overview;
- Architectural Diagram (hardware, software, and network configuration);
- Access Authorization Matrix;
- Data Classification;
- Standards Compliance;
- Standards Exceptions, Risks and Mitigating Controls;
- Change Management procedures;
- Business Continuity Planning;
- Testing Schedule and Target Production Date;
- Sign-off by:
  - Owner
  - Project Manager
  - Agency security staff

5.1 Projects which DO NOT Require State of Kansas Resources, Systems or Network Connections

Projects which do not require State of Kansas resources, systems, or connections to State of Kansas controlled networks, do not require review and recommendation by State of Kansas agency security staff, however, they must develop a security plan which shows all State information is being protected.

5.2 Projects which Require State of Kansas Resources, Systems, or Network Connections

The agency security staff should be contacted in the beginning phase of each project. Projects requiring State of Kansas resources, systems, or network connections must work with the DISC Bureau of Telecommunications for network design and the agency security staff to develop a security plan. The Agency security staff will review the plan and make recommendations to the Project Manager or author. The Agency security staff may, at their discretion, not review or make recommendations about security plans where the project is already in production and/or where it presents low risk. The Project

Manager must then obtain sign-off by the owner and the Agency security staff prior to production, and/or before any network connectivity as described above.

5.3 Security Implications for System Development and Testing

Appropriate information security and audit controls shall be incorporated into all new systems. Each phase of systems development and testing shall incorporate corresponding assurances of security and audit controls. The ultimate responsibility for insuring appropriate levels of security and audibility lies with the application owner. In conjunction with the application developer, the owner must define the level of security for each phase based on the sensitivity and criticality of the data being processed. In absence of a methodology, the following information should be considered during system development and testing.

- The test functions should be kept either physically or logically separate from production functions.
- Copies of production data shall not be used for testing unless the data has been declassified or unless all personnel involved in testing are otherwise authorized access to the data.

The following security activities should be addressed at the appropriate phase in system development or acquisition of new information processing systems:

1. Determine sensitivity and criticality of the system information and define security objectives, i.e., assess the threats, vulnerabilities, and risks to the system.
2. Identify security alternatives and basic security framework in the selected system architecture.
3. Define security requirements and select appropriate controls.
4. Develop security test plans.
5. Include approved security requirements and specifications in the development baselines.
6. Conduct tests of security in the configured components and in the integrated system.
7. Prepare documentation of security controls and assign to the documentation the appropriate level of sensitivity.
8. Conduct acceptance test and evaluation of system security.

After a new system has been placed in operation, all program changes shall be approved before implementation to determine whether they have been authorized, tested, and documented.

1. A naming standard should be in effect to distinguish between test jobs and production jobs, test data sets and production data sets.
2. Change control procedures should ensure that all moves between the test and production environments have been authorized in writing by the appropriate manager.
3. Parallel or acceptance tests should be considered production work and therefore run by production personnel.
4. Program development personnel should access production data and production program files only to resolve emergencies. Only those authorized by the supervisor of production operations should authorize and log this access.
5. All programs should be installed into production from the source code (i.e., programs will be recompiled by a change control or comparable group).

6. Software generally referred to as “public domain” software (such as might be acquired through software exchanges or electronic bulletin boards) or software not acquired under license or contract should never be used for processing confidential or sensitive information.
7. Acceptance testing of modified programs should be performed by a quality assurance (or independent) function using control test files.
8. Only authorized personnel should apply program changes, catalog and copy newly updated programs to production libraries.
9. Automated logs should be used to monitor all access to password tables and production programs.

6. Information Security

Protecting State of Kansas’s information assets is a process that incorporates many compensating controls. The State of Kansas requires that agencies identify, classify and protect the automated files, databases and applications it owns. Classifying information and the applications that function to process it is at the heart of identifying and selecting appropriate security and risk management practices. State of Kansas's security objectives must include maintaining information integrity and confidentiality while assuring the availability of critical information technology support services.

6.1 Authorized Use and Ownership of Information Resources

All information and telecommunication resources leased or owned by State of Kansas and all processing services billed to State of Kansas are to be used to conduct company business except as otherwise provided by management directives.

All computer software programs, applications, source code, object code, and documentation is State of Kansas property and will be protected as such if developed either:

- by State of Kansas employees in the course and scope of their employment or with the use of State of Kansas equipment, materials, or other resources; or
- by contract personnel acting under a contract with State of Kansas, unless the contract under which the software or documentation is developed specifically provides otherwise; or
- With State of Kansas funds.

All computer software programs, applications, and documentation purchased for the use of State of Kansas is State of Kansas property and will be protected as such.

It is a violation of State of Kansas policy to copy proprietary software in violation of a licensing agreement.

6.2 Availability of Critical Data & Systems

The State of Kansas, Executive Branch Chief Information Technology Officer requires agencies to have a Business Continuation Plan that includes the procedures necessary to assure the continuation of vital State operations in the event of a disaster. Each agency of the State of Kansas must identify and prioritize its processes.

The Business Continuation Plan must outline the internal policies and procedures that are to be employed should a disaster occur. Preparation of the recovery strategies for all time-sensitive processes must be coordinated with the agency's Business Continuation

Manager. In the event of a disaster all time-sensitive services, systems and applications must be restored and available on a priority basis to maintain vital State operation.

Time-sensitive applications include those systems whose loss or unavailability is unacceptable to the citizen's of Kansas. The loss or unavailability of support services provided to these applications may adversely affect the continuation of vital programs and services or the fiscal or legal integrity of State of Kansas operations.

6.3 User Accountability: Userids and Passwords

Passwords and Userids are pre-stored combinations of characters used by the host computer to authenticate the identity of an individual. Based on these the computing system can restrict or grant specific privileges.

Properly implemented and managed, userids and passwords will improve the likelihood that users are who they purport to be and that a user's access can be controlled effectively. Both are important deterrents to intrusion.

Each user of a multiple-user automated system shall be assigned a unique personal identifier or userid. User identification shall be authenticated before the system may grant that user access to automated information.

A user's access authorization will be removed from the system when the user's employment is terminated or the user transfers to a position where access to the system is no longer required.

Passwords must be:

- individually owned;
- kept confidential;
- changed whenever disclosure has occurred or may have occurred, and changed at least every 60 days;
- changed significantly (i.e., not a minor variation of the current password);
- A minimum of six characters and contain alphanumeric characters.

Passwords must not be:

- shared with other users;
- repeated for at least two cycles of change;
- repeating sequences of letters or numbers;
- names of persons, places, or things that can be closely identified with the user (i.e., spouse, children or pet names);
- the same as the userid;
- Stored in any file program, command list, procedure, macro or script where it is susceptible to disclosure or use by anyone other than its owner.

6.4 Access Controls

Information access control systems are a means of safeguarding the information assets of agencies of the State of Kansas. The following points help identify attributes of an effective information access control system.

- Authority to read, write, modify, update, or delete information from automated files or databases should be established by the owner(s) of the information. Individuals may be granted a specific combination of authorities. For example,

an individual may be allowed to “read only” or to “read and write but not delete” data. Specific access authority should be established on a need to know basis.

- Security administration should not require programmer intervention.
- Identification should be unique for each user of the system.
- The system should provide a method to validate the user is who he/she purports to be (e.g., passwords, smart tokens, and smart cards).
- Enforcement of strong password controls.
- Authorization to information should be specific as to who is allowed access and what information can be accessed.
- Security administration activity should be recorded and reviewed and security violations should be detected and reported.

6.5 Authorization

State of Kansas computing systems must provide the means to explicitly allow access to specific information when necessary. Authorization must be specific as to:

- who or what is allowed access (e.g., person or another computer system or device);
- What information may be accessed?

Systems must be able to limit a user’s access to only the information required to perform authorized work assignments (e.g., separate inquire from update capabilities, sensitive versus non-sensitive functions).

6.6 Audit Trails

Audit trails must be maintained to provide accountability for all security administration activity. Systems must record and report security administration activity as well as detect and report security violations. Systems should also provide a means to recover current and historical information about security administration activities in the event of a system failure.

The system must not disclose passwords through reporting functions.

Automated chronological or systematic records of changes to data are important in the reconstruction of previous versions of data in the event of corruption. These records are useful in establishing normal activity, identifying unusual activity, and in the assignment of responsibility for corrupted data.

A complete history of transactions will be maintained for each session involving access to confidential/protected nonpublic information to permit an audit of the system by tracing the activities of individuals through the system.

In addition to system start-up and shutdown times, transaction histories should log the following information:

- update transactions;
- date, time of activity;
- user identification;
- sign-on and sign-off activity; and
- Confidential/protected nonpublic display transactions.

Only designated personnel should have access to the transaction histories and to the results of any analyses.

Security Administration and data owners will conduct regular reviews of audit logs to detect any unusual or inappropriate activity. In addition to checks against authorizations, particular attention should be paid to unusual times, frequency, and length of accesses, as well as irregularities that could indicate potential violations.

6.7 Application Security

Network access to an application containing private, nonpublic, confidential, or protected nonpublic data, and data sharing between applications, shall be as authorized by the application owners and shall require authentication.

The owner of applications containing non-critical or non-sensitive data should likewise establish criteria for access and user validation, particularly on systems authorized for public use.

6.8 Adapting Policies and Procedures

State of Kansas programs and supporting computer applications frequently undergo modifications that may affect an existing security system. To ensure that security issues are considered when changes do occur, system documentation should address the impact modifications may have on the existing security system. Security procedures should ensure that the security system and its supporting documentation are periodically reviewed and, if need be, corrective action is planned for and implemented.

7. Authentication, Data Encryption & Key Management

7.1 Authentication

Authentication techniques function to protect information by controlling access to the assets of a data processing system. Authentication techniques permit validation of people's identities, hardware devices, and/or transmitted information. Validating or authenticating data and/or the identities of users, terminals, computers, and peripheral devices within a data processing system is vital to the protection of the information the system processes.

Authentication schemes are based on the possession of specific knowledge, capabilities, or personal attributes. They function as challenge-response mechanisms and include password, smart card/token processing, message authentication, and biometric techniques. Having and supplying the correct information authenticates an individual to the data processing system. Similarly, a computer, terminal, or other peripheral may be authenticated as an authorized device of a data processing system. Having and supplying the correct information when it is requested by an authorization system authenticates a device to the system.

Systems should implement authentication functions that are consistent with the level of confidentiality or sensitivity of the information they contain and process. When considering authentication techniques, first determine if the confidentiality and/or criticality of the information processed by the system requires stronger authentication than passwords alone. If so, the appropriate authentication device should be considered.

7.2 Devices

Several types of authentication devices are available which permit the process of authentication to be inexpensively strengthened. The two most common types of authentication devices are the smart card and the smart token. Both devices strengthen the authentication process by providing its user with a unique computational capability or additional secret information.

The smart card is a passive device that requires a separate reader for operation. The smart token is an active device with keyboard and display. Both devices function in a cooperative challenge/response protocol with system authentication software.

7.3 Services

Third party authentication services are implemented as specialized secure servers in networks employing the client/server architecture. These servers are used to authenticate clients and their respective servers to each other in a manner that avoids passing readable authentication information across the network.

7.4 Encryption

Encryption is the process of character substitution or transposition in a sequence determined by an encryption formula. Most encryption uses the Data Encryption Standard (DES) formula, which has been endorsed by the National Institute of Standards and Technology. Readable text is converted to unreadable text, called cipher text, based on a security key provided by the owner of the information. Anyone examining an encrypted file would see a string of unrelated characters or symbols. The encryption process can be reversed or decrypted only by someone who has the security key.

Data encryption techniques are used to control access to information, protect the integrity of transactions, disguise data during transmission, and authenticate the users and devices of an information processing system.

7.5 Encryption Requirements

The need for encryption is determined by the classification of the information and the location of the information. Information which travels over public networks requires encryption.

DATA ON INDIVIDUALS	**PUBLIC**	**PRIVATE**	**CONFIDENTIAL**
DATA NOT ON INDIVIDUALS	**PUBLIC**	**NONPUBLIC**	**PROTECTED NONPUBLIC**
Storage on fixed media	Unencrypted	Unencrypted provided logical access is limited	Encrypted unless stored on an isolated system in a physically secured area and logical access is limited
Storage on exchangeable media	Unencrypted	Encryption optional provided logical and physical access is controlled	Encrypted or physical access to media securely controlled;logical access limited
Transmission over a wide area network	Unencrypted	Encryption required	Encryption required

(WAN)			
Transmission over a local area network (LAN)	Unencrypted	Encryption optional at owner's discretion	Encrypt unless on an isolated network in a secured area
Transmission by FAX	Unencrypted	Encryption recommended but not required	Encryption required

7.6 Encryption Services

The table below contains the security services that may use encryption, a definition of the service, and encryption methodologies currently being used at the State of Kansas.

SECURITY SERVICE	DEFINITION OF SECURITY SERVICE	ENCRYPTION METHODOLOGY USED AT THE STATE OF KANSAS
Confidentiality Protection	Protection from revealing information to unauthorized entities or individuals.	
Integrity Protection	Preventing data from being modified or manipulated from its original state. In some cases, only integrity protection may be required, then confidentiality protection would not be required.	
Non-repudiation Protection	The ability to demonstrate to a third party that the originator of a transaction did, in fact, originate that transaction and that the message was not modified.	

7.7 Considerations for Data Encryption Systems

The costs associated with a hardware and software data encryption system vary greatly. With respect to the benefits and costs associated with a data encryption system, consider the following:

- What value is attached to the information to be protected?
- Is the information confidential or sensitive?
- What risks are associated with its unauthorized access or undetected modification?
- How long does the information need to be secured (i.e., minutes, hours, days, or years)?
- What are the development, operational, and overhead costs associated with the data encryption system?

? Identify the (1) installation costs, (2) hardware/software costs, (3) personnel training costs, (4) costs associated with changing keys, and (5) system maintenance costs.

7.8 Encryption and Authentication Keys

Encryption techniques can be divided into two general categories, symmetric or private key techniques and asymmetric or public key techniques. In private key encryption, the receiver of a message uses the same key to decrypt the message as the sender used to encrypt the message. Public key encryption provides both the sender and receiver with two keys, one private and one public. Private keys are the secret of their users, while public keys are openly available via a directory. When public key encryption is used, the sender encrypts the message in the public key of the intended receiver. Upon reception, the message is decrypted with the receiver's private key. Public key encryption technology simplifies the processes of key distribution and implementation of authentication functions.

7.9 Key Management

The functions associated with generating, distributing, storing, protecting, and destroying authentication and data encryption keys are collectively referred to as key management. Without adopting internal policies and procedures that address key management issues, a company risks serious security problems. Specifically:

? an unauthorized individual possessing the key and having access to encrypted data might have access to confidential or sensitive information;
? losing the key will render the company unable to read or process encrypted data; and,
? The company cannot guarantee the security of its information.

Key management functions should be designed to protect authentication and data encryption keys and associated materials from unauthorized disclosure, substitution, insertion, deletion, and recording. Unauthorized attempts to access key management information should be detectable and unsuccessful.

7.10 Data and File Encryption

Properly implemented, an encryption system virtually eliminates risks of disclosure of sensitive information at network nodes and facilities that are not under State of Kansas control, such as the public switched network. Encryption also protects against undetected modification of data and thus enhances integrity as well as confidentiality. Interception or modification of unencrypted information must be recognized as a significant threat.

Security through encryption depends upon both of the following:

? proper use of an approved encryption methodology, and
? Only the intended recipients holding the encryption key-variable (key) for that data set or transmission.

7.11 Guidelines for data and file encryption:

1. In making the determination to use data and file encryption, the following risks should be considered:

- loss of State of Kansas funds;
- violation of individual expectations of privacy;
- violation of state or federal law;
- civil liability on the part of State of Kansas;
- compromise of State of Kansas legal or investigative efforts;
- loss of business opportunities for affected persons; and
- Undue advantage to any person in State of Kansas competitive business relations.

2. Interception of unencrypted information may not be readily detectable. It should be assumed that unencrypted information is available to any determined intruder.
3. When encrypted data is transferred between organizations, the respective Information Resource Managers should devise a mutually agreeable procedure for secure key management. In the case of conflict, the data owner should establish the criteria.
4. Keys should be communicated separately from the encrypted information, preferably through different channels.
5. Passwords and dial-up terminal identifiers should be encrypted during transmission and in storage. They should be encrypted during session logon if the information to be exchanged requires encryption.
6. Encryption and decryption devices should be located as near the using devices (connected terminals and processors) as possible to minimize the need for other safeguards on the unencrypted segments of the link.
7. Sensitive or critical information should be stored in encrypted form if physical controls are not sufficient. Volumes or files where all sensitive information is encrypted may be controlled as though the information is not sensitive as long as encryption keys are appropriately controlled.
8. Security through encryption may be enhanced by requiring that two trusted individuals control the key; each having custody of half the key.

8. Network Security Policies

There are two types of access: trusted and untrusted. Trusted access refers to access between State of Kansas controlled nodes, systems, or networks. Untrusted access refers to access between non-State of Kansas controlled nodes, systems, or networks and State of Kansas controlled nodes, systems, or networks.

In addition to the types of access, there needs to be considerations for public vs. private networks. Public networks are defined as those accessible to the general public, such as: the Internet, telephone lines, satellite links and wireless or cellular communications. Public networks are considered untrusted. Therefore, all restrictions as applied to untrusted will be applied to public. Private networks are defined as networks not available to the general public such as any State of Kansas Local or Wide Area Network. Private networks may only be considered trusted if the network is controlled from end to end by State of Kansas.

8.1 General Network Controls

Network resources participating in the access of confidential/protected nonpublic information shall assume the confidentiality level of that information for the duration of the session. Controls shall be implemented commensurate with the highest risk.

All network components under State of Kansas control must be identifiable and restricted to their intended use. Following are some guidelines:

1. Password protected screen savers, terminal lock and key, or terminal software locking options should be enabled on each terminal so that access can be controlled by locking the terminal while it is unattended. This type of protection is particularly important at locations where access to the network during non-business hours is not tightly controlled.
2. All line junction points (cable and line facilities) should be located in secure areas or under lock and key.
3. Control units, concentrators, multiplexers, switches, hubs and front-end processors should be protected from unauthorized physical access.
4. Procedures should be implemented which ensure that access to data or information is not dependent on any individual. There should be more than one person with authorized access.
5. Some types of network protocol analyzers and test equipment are capable of monitoring (and some, of altering) data passed over the network. Use of such equipment should be tightly controlled since it can emulate terminals, monitor and modify sensitive information, or contaminate both encrypted and unencrypted data.

8.2 Distributed Network Access Security

State of Kansas owned or leased network facilities and host systems are State of Kansas's assets. Their use should be restricted to authorized users and purposes. Where public users are authorized access to networks or host systems, these public users must be clearly identifiable and restricted to only services approved for public functions. State of Kansas employees who have not been assigned a userid and means of authenticating their identity to the system are not distinguishable from public users and should not be afforded broader access.

Owners of distributed information resources served by distributed networks shall prescribe sufficient controls to ensure that access to those resources is restricted to authorized users and uses only. These controls shall selectively limit services based on:

- user identification and authentication (e.g., password, smart card/token); or,
- designation of other users, including the public where authorized (e.g., public access through dial-up or public switched networks), for the duration of a session; or,
- Physical access controls.
- Software patches or hardware changes made to network resources to maintain security must be reviewed periodically to assure that they are maintained properly.

8.3 Guidelines for distributed network access:

1. For distributed processing systems and local area networks, authorization at network entry should be made on the basis of valid user identification (e.g., userid) and authentication (e.g., password, smart card/token).
2. The host security management program should maintain current user application activity authorizations through which each request must pass before a connection is made or a session is initiated.
3. Unauthorized attempts (successful or otherwise) to access or modify data through a communication network should be promptly investigated.
4. If unauthorized access or modification of data occurs, the agency should promptly review its existing security system, including its internal policies and procedures. Appropriate corrective actions should be planned for and

established to minimize or eliminate the possibility of reoccurrence. Employees may need to be reminded of existing or revised procedures.

8.4 Network connectivity and Monitoring Controls

	CONTROL NAME	CONTROL STANDARD
1.	Connections	No communication device router, gateway or other network may be connected to a State of Kansas network without approval from the DISC Bureau of Telecommunications and the Agency security staff. All communications design architectures, connecting to the State of Kansas network, must also be reviewed and approved by the DISC Bureau of Telecommunications.
2.	Addressing	Network names and addresses should be coordinated by a central addressing authority.
3.	System and Node Authentication	Each system and node in a network must authenticate each accessing user, process, or other entity. This may be either through individual logon or by means of a single sign-on to a strongly authenticated State of Kansas agency controlled security server. Connection paths, terminal addresses, node addresses or other identifiers do not constitute an acceptable means of user authentication.
4.	Trusted Node Authentication	The use of trusted nodes requires that the owners of all participating nodes agree to the adequacy of the controls for authentication of users of those nodes. Participating nodes must also authenticate the identities of other nodes. Connection paths, terminal addresses, node addresses or other node identifiers do not, by themselves, constitute an acceptable means of node authentication. Only State of Kansas owned, operated, and controlled nodes located in restricted facilities may be trusted nodes.
5.	Network Diagnostic and Monitoring Tools	Possession, distribution or use of network diagnostic, monitoring, and scanning tools such as LAN analyzer and attack scanners (both hardware and software) is limited to designated and authorized personnel in accordance with their job responsibilities. This includes anything that can replicate the functions of such tools. Unauthorized possession, use, or distribution of such tools or functions is prohibited and may be grounds for immediate dismissal.

6.	IP Address Classification	IP addresses for firewalls and other security servers are classified as protected nonpublic, therefore, the appropriate classification guidelines should be followed.

8.5 System Identification Screens

State of Kansas system identification screens may include the following warning statements:

- ? Unauthorized Use is Prohibited;
- ? Usage May be Subject to Security Testing and Monitoring; and
- ? Abuse is subject to criminal prosecution.

8.6 Guidelines for system identification screens:

1. The system identification screen should be implemented so that it cannot be bypassed by a user.
2. The system identification screen should remain on display for a sufficient amount of time for the message to be read.
3. If the system cannot display an identification screen with an appropriate warning message, the message should be included on a printed label affixed to each video display terminal.

9. Personal Computers and State of Kansas Equipment Policies & Guidelines

Information is an important State of Kansas asset requiring appropriate protection. Measures must be taken to protect information from unauthorized modification, destruction or disclosure, whether accidental or intentional, as well as to assure its security, integrity, availability, and confidentiality.

Excessive personal use of State of Kansas's computer equipment or any inappropriate use of the same may subject the employee to disciplinary action up to and including termination of employment.

9.1 Practices

9.1.1 Information Security

All information must be identified and classified according to its level of security confidentiality and business "need-to-know." Know the classification of the information that you are responsible and with which you work. Classifications are:

1. Data on Individuals:

- ? Public – any information that can be disclosed to anyone for any reason without violating an individual's right to privacy;

- Private – information on an individual that can be disclosed to the individual, anyone authorized by the individual, or by law;
- Confidential – information intended solely for use within State of Kansas and limited to those with business need-to-know.

2. Data Not on Individuals:

- Public – data that can be disclosed to anyone for any reason without violating an individual's right to privacy;
- Nonpublic – data available only to the data subject and anyone authorized by the data subject or by law;
- Protected Nonpublic – information intended solely for use within State of Kansas and limited to those with business need-to-know.

Do not disclose information that is classified as not public to unauthorized persons. Always verify the identity and the need-to-know of anyone requesting this information. Notify your management of unauthorized attempts to obtain information.

9.1.2 Visual Displays:

To prevent someone from viewing information without your knowledge, take precautions such as:

- using a screen saver on your computer monitor;
- erasing white boards containing Confidential or Protected Nonpublic information; and
- immediately removing Confidential or Protected Nonpublic information from printers or facsimile machines; and
- Removing and securing Protected Nonpublic information from your desktop.

9.1.3 Wireless Transmissions:

Do not discuss or transmit Confidential or Protected Nonpublic information on unencrypted cordless telephones, cellular phones or wireless modems because conversations can be easily intercepted and monitored. Never discuss or transmit Confidential or Protected Nonpublic information without explicit authorization.

9.1.4 Passwords

See Section 6.3 for a detail discussion of userids and passwords.

9.1.5 Computer and Network Security

Take the following precautions to prevent unauthorized individuals from gaining access to State of Kansas information and systems:

- protect your personal authenticators (passwords, PINs, smart cards, tokens, etc.) so they cannot be used by others;
- do not disclose or share passwords with anyone, including your management;
- do not leave your workstation unattended while logged on without some type of access control (i.e., password protected screen saver); and
- Notify your management and NOC if you detect any unauthorized use or attempted misuse of your personal authenticators, terminal sessions or equipment.

9.1.6 Anti-virus Software:

You must use virus detection and eradication software to scan for viruses. Scanning should be performed:

- during system start-up;
- when a disk is inserted;
- after software installation; and
- Before loading programs obtained from external sources (for example, the Internet, vendors or bulletin boards).

Additionally, auto protect features should be enabled to scan a file when it is opened, saved or executed. See section 11.7 for additional virus protection information.

9.1.7 Data backup and Storage:

Routinely make duplicate copies of information. Store original software programs and backup data copies in a secure place.

9.1.8 Portable Computers:

Do not leave portable computers unattended; lock them up when they are not in use. In addition:

- portable computers containing Private or Nonpublic information should use software access controls and anti-theft devices; and
- Portable computers containing Confidential or Protected Nonpublic information should use encryption software.

9.1.9 Remote Access:

Dial-in access to State of Kansas should be established through the dial-up access to the Kanwin network. The use of individual modems connected to single PCs, terminals, or servers provide unprotected "back doors" to the entire State network and must not be permitted by individual agencies without specific protective measures.

9.1.10 Diagnostic and Monitoring Tools:

Distribution or use of network diagnostic, monitoring, scanning tools or hardware/software attack scanners is limited to designated and authorized personnel. If you distribute or use these tools without authorization, it can result in your immediate termination.

9.1.11 External Systems

If you have access to the Internet or any other external systems, be sure to follow all appropriate information security policies. For example:

- ? do not transmit information belonging to State of Kansas outside the agency without appropriate approvals and precautions;
- ? remember that e-mail and data sent to or received from external systems, such as the Internet, are not secure or private and are easily readable; and
- ? Never download and start any programs until you have verified they are not contaminated with a virus.

9.1.12 Software and Licensing

Only State of Kansas-approved software should be used. All software must be owned by State of Kansas or properly licensed to State of Kansas by the owner of the software.

9.1.13 Privacy

Files and messages you send or receive using company computing resources and equipment are not private communications. If necessary for job-related reasons, authorized State of Kansas personnel may inspect and monitor the company's computing resources and equipment at any time. The company does not regularly monitor such communications, but reserves the right to do so.

9.1.14 Security Incident Reporting

If a computer is stolen, or if company information is modified, destroyed or taken in an unauthorized action, notify your manager and NOC immediately.

10. Physical Security

Physical Security should consider identification of sensitive areas, identification of entry and exit points, access authorization (procedures and monitoring devices, alarms), assessment of nearby businesses, natural disaster-prone areas, electrical supplies, manmade threats, specific information system environmental controls, etc.

The following practices must be adopted in order to maintain adequate Physical Security within State agency offices

10.1 Access control measures:

1. All servers and other sensitive pieces of hardware should be kept in locked rooms.
2. Wiring closets should be kept locked at all times.
3. Secure Storage for laptop computers should be available within all State agency offices.
4. Laptop computers that are used outside the office and that contain confidential information should have some means of protecting the data, such as encryption or maintaining the data on removable disks.
5. All computer rooms and Telecommunication distribution frames must be located in rooms with card key access. In addition, access control measures for raised floor computer rooms must include the following.

    a. Walls separating work areas on raised floor where the level of security is different on either side of the partition must extend and completely shut off the area between the raised floor and the permanent floor.

    b. Only persons whose work requires them to be in raised floor computer rooms on a day to day basis will be granted access cards to those areas.

    c. All visitors to computer room facilities must sign in at the security access point.

    d. Logs of all visitors to computer rooms will be maintained for a minimum of 1 year for audit purposes.

    e. Formal procedures must be established for the issuance and removal of card keys.

    f. The Data Center Manager is responsible for processing requests for new cards, changes to existing cards and deletions of card.

6. Whenever an employee leaves a State agency for other employment the immediate supervisor must obtain building passes, access card keys or similar articles. The supervisor must also notify the Data Center Manager immediately upon an employee's separation.

7. All State agencies must have policies and procedures in place for locking doors after work hours. All hub rooms, communications rooms for telecommunications and wiring closets must be secured with key locks, card keys or punch down locks.

10.2 Fire Suppression Measures

1. All State agency work areas must have hand held fire extinguishers available in accordance with published fire prevention standards for public access buildings. These extinguishers must be checked by a licensed extinguisher inspector on at least a yearly basis.

2. Care must be taken to properly store flammable solutions or materials

3. Fire doors are not to be propped open for any reason.

4. All State agency employees will participate in regularly schedule evacuation drills.

5. With regards to Raised Floor Computer Rooms:

a. Low Flame spread materials are to be used wherever practical in the construction of computer rooms

b. Dampers and Shutters are to be included in the heating and cooling subsystems of building housing computers that can be closed to slow the spread of fire.

c. Detection equipment must be included in the construction of computer rooms that activate alarms at a centrally located console area. This equipment must be tested on a regular basis.

d. Sprinkler systems in computer rooms must be of the “dry line” type to prevent accidental discharge of water on electronic equipment.

e. If dry chemical type extinguishing systems, such as Halon, are used in computer rooms, these systems are to be checked by qualified technicians on at least a yearly basis.

10.3 Environmental Measures.

1. With regards to Raised Floor Computer Rooms.

a. Adequate air handling equipment must be installed to insure room temperatures consistent with computer equipment needs. Redundancy should be included in this plan to accommodate times when primary equipment is down.
b. The area below the raised floor must be thoroughly cleaned at least on a yearly basis to prevent circulation of harmful dust particles.
c. Monitoring equipment must be installed to track temperature and humidity. This equipment must be capable of sounding an alarm should one of these environmental conditions exceed predetermined thresholds.

10.4 Electrical Power Measures

1. Uninterrupted Power Supply (UPS) systems must be utilized to assure continuous power to systems deemed critical to State of Kansas business.

2. Surge protection equipment should be utilized to protect electronic equipment that might be sensitive to power fluctuations.

3. Anyone working on or around electronic data processing equipment must wear static electricity eliminating bracelets.

10.5 Office space

1. All State Agencies must have policies and procedures in place for locking doors after work hours.

2. All hub rooms, communications rooms for telecommunications and wiring closets must be secured with key locks, card keys, or punch down locks.

11. Issue-Specific Policies

11.1 User Responsibilities

Users are responsible for any and all activity initiated by their e-mail ID, userid or personal workstation.

Individuals must not disclose internal State of Kansas information via the Internet that may in any way adversely affect State of Kansas customer relations or public image.

State of Kansas private, nonpublic, confidential, or protected nonpublic information must not be sent over the Internet unless it has first been encrypted by a State of Kansas approved encryption method.

If sensitive State of Kansas information described in previous paragraphs is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties notify the Agency security staff immediately.

11.2 Internet Access

The Internet is notoriously insecure. State of Kansas employees and contractors should not send any data over the Internet in clear text. This data must be encrypted by approved, strong encryption software.

Access to and from the Internet represents potentially significant exposures to the State of Kansas network. Following are the minimum controls required to establish an Internet connection utilizing State of Kansas computing or networking resources. It applies to all individuals who use the Internet with State of Kansas resources as well as those who represent State of Kansas.

State employees must use good judgement in Internet access. Each use of the Internet must be able to withstand public scrutiny without embarrassment to the State of Kansas.

Examples of inappropriate Internet use include, but are not limited to:

- illegal activities;
- wagering, betting or selling;
- harassment and illegal discrimination;
- fund-raising for any purpose unless agency sanctioned;
- commercial activities (e.g., personal for-profit business activities);
- promotion of political or religious positions or activities;
- receipt, storage or transmission of offensive, racist, sexist, obscene or pornographic information;
- downloading software (including games, wallpaper, and screen savers) unless agency-sanctioned;
- Use by individuals other than State employees.

An individual's association with the State of Kansas may be disclosed in bulletin board discussions, chat sessions, and other offerings on the Internet via the individual's e-mail address or other means. In these cases, the user must also clearly indicate that the opinions expressed are his/her own, and not necessarily those of the State of Kansas.

State of Kansas facilities and connections may not be used to make unauthorized connections to, break in to, or adversely affect the performance of other computer systems on the network. Access to other computer systems via the Internet does not convey the right to use or connect to these computer systems. This right only comes from proper authorization by the owners of those computer systems. Individuals must not "test the doors" or "probe" security mechanisms at either State of Kansas or other Internet sites unless they have first obtained permission from the Agency security staff.

11.2.1 Monitoring Internet Access

State of Kansas reserves the right to monitor all use of Internet resources at the time of use, during routine post-use audits, and during investigations. Any investigations that uncover improper Internet use may result in disciplinary action up to and including termination.

11.3 E-mail

Many agencies of the State of Kansas maintain electronic-mail (e-mail) systems to assist in conducting State of Kansas business. These systems, including the equipment and the data stored on the equipment, is at all times, the property of the State of Kansas.

The State of Kansas cannot guarantee the privacy of electronic communications because electronic communications are not private by nature, and are inherently insecure. Even though passwords might appear to provide confidentiality, privacy of messages cannot be assumed. This means that e-mail could be read, altered, or deleted by unknown parties without the knowledge or permission of the worker who composed, sent, or received the message or its attachments(s). In addition, note that even when e-mail messages are deleted or erased, it could still be possible to recreate the original message.

An individual's association with the State of Kansas may be disclosed in bulletin board discussions, chat sessions, and other offerings on the Internet via the individual's e-mail address or other means. In these cases, the user must also clearly indicate that the opinions expressed are his/her own, and not necessarily those of the State of Kansas.

Periodic back-up of e-mail is encouraged. However, e-mail must be disposed of when no longer needed. Back-up and logs of e-mail server computers must be destroyed one year after being archived.

State of Kansas Agency management reserves the right to retrieve and review any message or attachments(s) composed, sent, or received. State of Kansas Agency managers and supervisors may review at any time the messages of workers they supervise in order to determine whether they have breached security, violated State of Kansas policy, or taken other unauthorized actions. Also, State of Kansas Agency management may disclose messages or attachment(s) to law enforcement officials without prior notice to the workers who may have sent or received such messages.

Managers and supervisors are responsible for ensuring the appropriate use of all electronic tools, including e-mail access through training, supervising, coaching. Improper use of State of Kansas e-mail could result in disciplinary action up to and including termination.

11.4 Voice Mail Systems

Voice mail may be used to receive and retrieve messages when employees are unable to answer their telephone. This communications device is usually connected to the telephone switches through call routing via extensions and the potential for unauthorized message receiving or fraudulent calling can occur.

The following steps should be taken to minimize fraudulent use of voice mail.

1. Never allow external incoming calls to be transferred to outside lines.
2. Use strong initial passwords and require that they be changed upon login.
3. Never use easy or obvious passwords and change them often.
4. Unassigned mailboxes should be deleted.
5. Monitor activity logs for repeated login attempts to specific mailboxes or to repeated random login attempts.
6. Lock the mailbox after 3 unsuccessful login attempts.
7. Require users to create personal greetings when setting up their mailbox.

11.5 Remote Access

Dial-up access via a modem poses a high risk of possible intrusion to State of Kansas networks. At the same time remote access conveniently enables State of Kansas employees, contractors and vendors to access State of Kansas computer resources from offsite locations.

State of Kansas networked systems, including mainframes, should not be accessed over the Internet using State of Kansas assigned logonids unless passwords are encrypted. Other protected transmission means such as the dial-up facilities must be used instead.

The use of individual modems connected to single PCs, terminals, or servers provide unprotected "back doors" to the entire State network and must not be permitted by individual agencies without specific protective measures.

11.6 Video

Video conferencing capabilities are offered to the entire State through the KANSAN network. This service is being used for classroom training, meetings, and public hearings as well as confidential hearings. Following are requirements for video conferencing:

- Point-to-point and multipoint video connections are made through State of Kansas's Network Control Center (NCC).
- No unauthorized recordings will be made of any videoconferences.
- There will be no unauthorized play back of authorized conference recordings.
- DISC employees responsible for administering connections for video conferencing will not record, play back or listen in on conference calls unless they are instructed to do so by the hosting party of the video conference.

11.7 Virus Protection

Computers infected with viruses or malicious code could jeopardize information security by contaminating data. This policy provides controls to protect against such attacks. Please refer to Information Security Incident Reporting information in section 4 for appropriate action for detected or suspected viruses.

A typical virus is a small computer program that, as part of its operations, reproduces itself by making copies of itself and inserting these copies into uninfected programs or data files. This insertion process takes only a fraction of a second, a virtually undetectable delay. The infected program will subsequently execute the virus code during its normal processing. In addition to its ability to reproduce, the virus may cause damage to the programs, data, or equipment, or it may perform some other function that is relatively harmless. Viruses can use one or more technique to achieve their purpose. Sharing data files can spread them. Personal computing environments are more susceptible to viruses, however, they can occur in the mainframe-computing environment as well. The following are controls that can reduce the chance of virus infection within the personal computing environment.

	CONTROL NAME	CONTROL STANDARD
1.	Virus Detection Software	Virus detection or integrity checking software should be used in all PC/LAN environments, including portable PCs and PCs located at employees' homes.
2.	Updating Virus Detection Software	The data files used by the detection software must be updated at least once a month to ensure system scans can identify most known viruses. A program to monitor vulnerability lists must be Implemented on a regular basis.
3.	Loading Software	a) No unapproved software may be loaded on State of Kansas PCs or LANs. b) All software introduced into State of Kansas PC/LAN computing environments, including State of Kansas PCs that are located in employees' homes, must be known to be virus free. c) All PC/LAN computing environments into which State of Kansas software and/or data is introduced must be known to be virus free. d) Software distributed from any State of Kansas PC/LAN computing environment to another State of Kansas organization or a State of Kansas customer must be known to be virus free.
4.	Verifying software	Virus scans or integrity checks must be done prior to the first use of each executable file that is brought into the State of Kansas environment from untrusted environments, e.g. program fixes copied from vendors' bulletin boards or web sites.

5.	Scanning Removable Media	Virus scans or integrity checks must be done prior to the first use of each diskette (or other removable media) after the diskette has been out of a State of Kansas-controlled environment. Examples: Diskettes used in a PC at home, whether owned by State of Kansas or not. Diskettes used in a customer or vendor's computer.
6.	Scanning Frequency	Virus scans of permanent media must be done at least daily: a) On any server connected to a network, e.g. a server connected to a LAN. b) On computers used for distribution of files outside of , e.g. those used to send files to external customers, user groups, or vendors c) On any workstation that shares software with any other computer. d) On computers running an application for which the risk is medium or high for loss of data or loss of the application. Virus scans must be done at least weekly in all other situations.
7.	Scheduling Virus Scans	Whenever possible virus scans should be scheduled to occur automatically. (All files should be scanned before being loaded on the network and a weekly network scan should be scheduled as well.)
8.	Audit Records	Records must be kept that show scans occurred and the details of any findings from the scans. Note: Some scanning software provides customized logs.

Appendix A: Security Acknowledgement

The following is an example of an Employee Agreement that all State agencies should establish and maintain.

Employee Agreement to Comply With
(State Agency) Information Technology Security Policy

The State of Kansas is devoted to information security and employs specialists to maintain security. However, it is the responsibility of users to comply with all information security policies and procedures.

By signature below, the employee hereby acknowledges and agrees to the following:

1. Employee is a "user" as defined in the State of Kansas Information Technology Security Policy manual;

2. As a user, employee shall comply with security measures dictated by both "owners" and "custodians," as defined in the State of Kansas Information Technology Security Policy;

3. Employee is a State of Kansas employee in possession of State of Kansas information resources;

4. Employee shall protect these information resources from unauthorized activities including disclosure, modification, deletion, and usage.

5. Employee has read and agrees to abide by the "State of Kansas Information Technology Security Policy" manual.

6. Employee agrees to discuss with a supervisor regarding policies or procedures not understood.

7. Employee shall abide by the policies described as a condition of continued employment.

8. Employee understands that any employee found to violate these policies is subject to disciplinary action, including but not limited to, privilege revocation and/or termination of employment.

9. Access to State of Kansas information systems is a privilege, which may be changed or revoked at the discretion of management.

10. Access to State of Kansas information systems automatically terminates upon departure from the State of Kansas employment.

11. Employee shall promptly report violations of these policies to the appropriate agency security office.

12. This document may be amended from time to time. The State of Kansas will notify employees of amendments. Employee will keep abreast of amendments to the "State of Kansas Information Technology Security Policy," as made available by hard copy or on-line.

ACKNOWLEDGMENT: STATE OF KANSAS INFORMATION TECHNOLOGY POLICY

_____ _____

User's signature Date Witness Date

_____

User's name in block capital letters

Appendix B: Glossary of Terms

Access: To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.

Access control: The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

Access password: A password used to authorize access to data and distributed to all those who are authorized similar access.

Account: A set of privileges for authorization to system access, which are associated with a userid.

Authentication: Verifying that a user is who he or she purports to be.

Authorization: The process of granting privileges to an authenticated user or entity.

Algorithm: A mathematical process for performing a certain calculation; in the information security field, generally used to describe an encryption process.

Brute force attack: An attack against an encryption algorithm where the attacker attempts to recover the secret key by trying all possible values. Longer keys are more resistant to brute force attacks.

Business need-to-know: A security concept which limits access only to information and information processing resources required to perform one's normal business related duties.

Business resumption: The ability to resume business after an outage. This is critical to our ability to service our customers.

Challenge/Response Password: A one-time password generating device, token, or SmartCard used in place of a reusable password.

Change management: Change management is documented procedures used to control the revision of applications and or operating systems in computing environments. These controls should involve a separate group (not the original programs) to control the changes to application and/or OS code.

Compliance statement: A document used to obtain a promise from a computer user that the user will abide by system policies and procedures.

Confidential information: A classification for information, the disclosure of which may damage the State of Kansas, Department of Administration, citizens of Kansas, or other involved parties.

Control Statement: A statement that applies to information which informs the user of special requirements, restrictions or protection.

Critical information: Any information essential to Department of Administration's activities, the destruction, modification, or unavailability of which would cause serious disruption to Department of Administration's mission.

Cryptography: The use of an algorithm to encrypt and/or decrypt.

Custodian: Guardian or caretaker; the holder of data; the agent charged with the resource owner's requirements for processing, telecommunications, protection controls, and output distribution for the resource.

Data: A representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means.

Data integrity: The state that exists when computerized information is predictably related to its source and has been subjected to only those processes which have been authorized by the appropriate personnel.

Data security or computer security: Those measures, procedures, or controls, which provide an acceptable degree of safety of information resources from accidental or intentional disclosure, modification, or destruction.

Decryption: The mathematical process by which an encrypted message is rendered readable or usable (reverses the encryption process).

Dial-in: The capability to allow one system to access information or receive a message from another system over non-dedicated public phone lines.

Dial-out: The capability to access information on another system and send a message. Dial-out occurs on the system that initiates the call.

Digital signature: A sequence of bits which accompanies a message that is generated via encryption; such a bit sequence shows that a message (a) was sent by an identified person, and (b) is free from modification or tampering.

Disaster: A condition in which an information resource is unavailable, as a result of a natural or manmade occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of agency program objectives, as determined by agency management.

Disclosure: Unauthorized access to confidential or sensitive information.

Dynamic password: A password which changes each time a user logs-into a computer system (typically accomplished via smart cards).

Encryption: The process of transforming readable text into unreadable text (ciphertext) for the purpose of security or privacy.

Encryption key: A secret password or bit string used to control the algorithm governing an encryption process.

End-user: A user who employs computers to support NAI activities, who is acting as the source or destination of information flowing through a computer system.

Exposure: The condition of vulnerability to loss resulting from accidental or intentional disclosure, modification, or destruction of information resources.

Firewall: A logical barrier stopping computer users or processes from going beyond a certain point in a network unless these users or processes have first passed some security test (such as providing a dynamic password).

Host Computer: Computer that provides a service or application that users access through a network connection. Historically the term has been used to refer to large mainframe computers.

In this document the term includes computers of any size and servers in client-server environments.

Information: That which is extracted from a compilation of data in response to a specific need.

Information resources: The procedures, equipment, facilities, software and data which are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

Isolated computer: A computer which is not connected to a network or any other computer; a stand-alone personal computer is an example.

Loginid: A character string that uniquely identifies a user on a computer system. This term is mainly used by NetWare.

Log-in script: A set of stored commands that can log a user into a computer automatically.

LogonID: A character string that uniquely identifies a user on a computer system. This term is mainly used in reference to a mainframe.

Network penetration: The attempt or successful act of bypassing the security mechanisms of a system.

Owner: The agent responsible for specific agency resources.

Password guessing attack: A computerized or manual process whereby various possible passwords are provided to a computer in an effort to gain unauthorized access.

Password-based access control: Software that relies on passwords as the primary mechanism to control system privileges and logging activities.

Password: Any secret string of characters which serves as authentication of a person's identity (personal password), or which may be used to grant or deny access to private or shared data (access password).

Privilege: An authorized ability to perform a certain action on a computer, such as read a specific computer file.

Privileged user-ID: A userid that has been granted the ability to perform special activities, such as shut down an application or system.

Production application: A tested, documented, and periodically-executed computer program which performs one or more regular business activities related to Department of Administration's mission; examples include accounts payable and payroll.

Retention schedule: A management-approved listing of the types of information that must be retained for archival purposes and the time frames that these types of information must be kept.

Risk: The likelihood or probability that a loss of information resources or breach of security will occur.

Risk analysis: An evaluation of system assets and their vulnerabilities to threats. Risk analysis estimates potential losses that may result from threats.

Risk management: Decisions to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

Router: A device that interconnects networks; used in some instances to provide access control and message routing services.

Security administrator: The person charged with monitoring and implementing security controls and procedures for a system.

Security controls: Hardware, programs, procedures, policies, and physical safeguards, which are put in place to assure the integrity and protection of information and the means of processing it.

Security incident or breach: An event that results in unauthorized access, loss, disclosure, modification or destruction of information resources whether accidental or deliberate.

Security standard: A required procedure or management control.

Sensitive information: Any information, the disclosure of which could damage NAI, business partners, customers, or other third parties.

Separation of duties: No one individual or function has control of entire process. When properly implemented, separation of duties provides the necessary checks and balances to mitigate against fraud, errors, and omissions.

Software macro: A computer program containing a set of procedural commands to achieve a certain result.

Strong, two-factor authentication: An authentication process using techniques which would require a high level of effort to compromise and are not subject to compromise by eavesdropping. The processes may employ cryptographic techniques in combination with repeated information such as reusable passwords. Strong authentication processes may use challenge/response password devices, SmartCards, or one-time passwords.

System administrator: A designated individual who has special privileges to maintain the operation of a computer application or system.

System control data: Data files such as programs, password files, security tables, authorization tables, etc., which if not adequately protected, could permit unauthorized access to information resources.

User: One that uses Information Technology resources of the Department of Administration.

Userids: Also known as accounts, these are character strings that uniquely identify computer users or computer processes.

Virus: A program (malicious code) which, when executed, copies itself onto other media or files available to the computer executing it.

Virus screening software: Commercially available software that searches for certain bit patterns or other evidence of computer virus infection.